HBSS 3.0 Classroom training V2



LEARNING HOST BASED SECURITY SOLUTION ESSENTIALS

**Overview of the HBSS Class:**

*What will the students learn?*

1. **Configure, and deploy McAfee Host IPS using ePO server 4.0**
2. **Understand the capabilities and features of HIPS.**
3. **Create General, Host IPS, Firewall polices and have a general understanding of Application Blocking policies**
4. **Create exceptions to allow essential processes to continue uninterrupted**
5. **Have an understanding of the proper way to tune policies within HBSS.**
6. **Working knowledge of the Assets, RSD and PA modules.**
7. **Perform security maintenance operations, administration tasks, and troubleshooting of HBSS.**
8. **Understand how to configure HBSS to meet CTO 07-12 mandate.**

This 4-day course is a System Administrator level, hands-on, *open-book* **tested course** that will cover the configuration and operation of the HBSS solution. Throughout the course, students will practice various policy configurations using VM-ware to simulate a student’s environment. Students will gain understanding of concepts and skills necessary to perform daily administration of HBSS in their network environment.

***Prerequisites for HBSS 3.0:***

***1.*** *HBSS administrator or equivalent*

***2.*** *Knowledge of the CTO 07-12 requirements*

***3.*** *Network and System administrator background*

HBSS 3.0 Class Administrative Items:

**Schedule**:

* Tuesday-Friday from 8am-5pm
* Lunch break from 11:30-12:30

**Dress Code**: Business Casual

**Homework**: To review the days materials and answer review questions

**Test**:

* 1 Hour Open Notebook Test on Friday.
* 35 Questions Students must get 25 Correct

**Evaluations**: Class evaluation forms will be handed out after class to be completed prior to leaving

**Certificate**: Tests will be graded while student is filling out the evaluation form. Student will receive a certificate before they leave class if they pass the test.

Course Outline:

1. Introduction to HBSS
2. Installation
3. Web-based Console and Dashboards
4. ePO Queries
5. ePO System Tree
6. ePO Sorting and Tagging
7. ePO Polices and Policy Catalog
8. ePO Users and Permission Sets
9. McAfee Agent
10. ePO Repositories
11. ePO Notifications
12. Rogue System Detection
13. HIPS\_Windwos Client
14. HIPS Ceneral Policy
15. HIPS IPS Policy
16. HIPS Firewall Policy
17. HIPS Application Blocking Policy
18. Solairs/ Unix Client
19. Assets Module
20. Device Control Agent
21. DLP User Assignments
22. Device Control
23. DLP Reporting
24. Policy Auditor

